



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

87

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/086,203	02/28/2002	Scott G. Ainsworth	0073512	9774
7590	12/02/2005		EXAMINER	
			ABYANEH, ALI S	
			ART UNIT	PAPER NUMBER
			2137	
DATE MAILED: 12/02/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/086,203	AINSWORTH ET AL.	
	Examiner Ali S. Abyaneh	Art Unit 2137	

— The MAILING DATE of this communication appears on the cover sheet with the correspondence address —

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 28 February 2002.

2a) This action is FINAL.                  2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-40 is/are pending in the application.

4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5) Claim(s) \_\_\_\_\_ is/are allowed.

6) Claim(s) 1-40 is/are rejected.

7) Claim(s) \_\_\_\_\_ is/are objected to.

8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 28 February 2002 is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All    b) Some \* c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____ .
3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>2-28-02</u> .	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____ .

**DETAILED ACTION**

1. Claims 1-40 are presented for examination.

**Information Disclosure Statement PTO-1449**

2. The Information Disclosure Statement submitted by applicant on 02-28-2002 has been considered. Please see attached PTO-1449.

***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 17, 21 and 37 are rejected under 35 U.S.C. 102(b) as being anticipated by Bisbee et al. (US Patent NO 5,748,738).

**Regarding claim 17**

Bisbee teaches a method for creating an authoritative electronic record in a repository, the method comprising the steps of: receiving an original electronic record in a repository; generating at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record (column 9, lines 66-67 and column 10, lines 1-7); prepending the first

receipt information at a beginning portion of the original electronic record (column 5, lines 55-67 and column 6, lines 1-13); generating at least some first identifying information, wherein the first identifying information includes a provable representation of the first receipt information (column 3, lines 12-21); appending the first identifying information at an end portion of the original electronic record (column 3, lines 33-35); and storing the original electronic record with the prepended first receipt information and the appended first identifying information in the repository as an authoritative electronic record (column 6, lines 43-59).

**Regarding claim 21**

Bisbee teaches a method for storing an original electronic record as an authoritative electronic record in a repository, the method comprising the steps of: transmitting an original electronic record to a repository (column 6, lines 14-16); allowing at least some first receipt information to be generated, wherein the first receipt information includes information relating to the original electronic record (column 6, lines 31-35); allowing the first receipt information to be prepended at a beginning portion of the original electronic record(column 5, lines 55-67 and column 6, lines 1-13); allowing at least some first identifying information to be generated, wherein the first identifying information includes a provable representation of the first receipt information (column 3, lines 12-21); allowing the first identifying information to be appended at an end portion of the original electronic record(column 3, lines 33-35); and allowing the original electronic record to be stored with the prepended first receipt information and the

appended first identifying information in the repository as an authoritative electronic record(column 6, lines 43-59).

**Regarding claim 37**

Bisbee teaches a system for creating an authoritative electronic record in a repository, the system comprising: a software program that is capable of receiving an original electronic record; a software program that is capable of generating at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record (column 9, lines 66-67 and column 10 lines 1-7); a software program that is capable of prepending the first receipt information at a beginning portion of the original electronic record (column 5, lines 55-67 and column 6 , lines 1-13); a software program that is capable of generating at least some first identifying information, wherein the first identifying information includes a provable representation of the first receipt information (column 3, lines 12-21); a software program that is capable of appending the first identifying information at an end portion of the original electronic record (column 3, lines 33-35); and a software program that is capable of storing the original electronic record with the prepended first receipt information and the appended first identifying information in the repository as an authoritative electronic record (column 6, lines 43-59).

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-16, 18-20, 22-36 and 38-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bisbee et al. (US Patent NO 5,748,738) in view of Vanstone (US Patent NO 6,212,281).

**Regarding claim 1**

Bisbee teaches a method in a computer system for maintaining and digitally signing a unique authoritative electronic record, the method comprising the steps of: receiving an original electronic record in a repository; generating at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record (column 9, lines 66-67 and column 10, lines 1-7); prepending the first receipt information at a beginning portion of the original electronic record (column 5, lines 55-67 and column 6, lines 1-13); generating at least some first identifying information, wherein the first identifying information includes a provable representation of the first receipt information (column 3, lines 12-21); appending the first identifying information at an end portion of the original electronic record (column 3, lines 33-35); storing

the original electronic record with the prepended first receipt information and the appended first identifying information in the repository as an authoritative electronic record; receiving a request to review and optionally sign the authoritative electronic record at a remote location; computing a complement of the proper subset of the authoritative electronic record; transmitting the complement of the proper subset of the authoritative electronic record to the remote location ( column 6, lines 14-59 and column 9, lines 27-41); displaying the complement of the proper subset of the authoritative electronic record at the remote location; allowing a digital signature to be computed at the remote location using the computed message digest and a private key (column 10, lines 23-49); returning the digital signature to the repository; receiving the digital signature in the repository; generating at least some second receipt information, wherein the second receipt information includes information relating to the signed authoritative electronic record (column 3, lines 12-21); prepending the second receipt information at a beginning portion of the signed authoritative electronic record; generating at least some second identifying information, wherein the second identifying information includes a provable representation of the receipt information; appending the second identifying information at an end portion of the signed authoritative electronic record; determining whether the digital signature information represents a valid digital signature (column 3, lines 23-37); and amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record in the repository to include the

digital signature information, the prepended second receipt information, and the appended second identifying information from the signed authoritative electronic record (column 6, lines 31-59). Bisbee does not explicitly teach computing a partial message digest of a proper subset of the authoritative electronic record; transmitting the partial message digest of the authoritative electronic record to the remote location and computing a message digest, at the remote location, using the partial message digest and the complement of the proper subset of the authoritative electronic record. However, in an analogous art, Vanstone teaches computing a partial message digest of a proper subset of the authoritative electronic record; transmitting the partial message digest of the authoritative electronic record to the remote location and computing a message digest, at the remote location, using the partial message digest and the complement of the proper subset of the authoritative electronic record (column 3, lines 55-67 and column 4, lines 1-26). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Bisbee's method to include computing a partial message digest of a proper subset of the authoritative electronic record; transmitting the partial message digest of the authoritative electronic record to the remote location and computing a message digest, at the remote location, using the partial message digest and the complement of the proper subset of the authoritative electronic record. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to

confirm authenticity, insure the accuracy of the message and furthermore to protect the individual blocks of data from any alteration (column 2, lines 45-49).

**Regarding claim 16**

Bisbee teaches a method in a computer system for maintaining and digitally signing a unique authoritative electronic record, the method comprising the steps of: providing for the receipt of an original electronic record in a repository; providing for the generation of at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record (column 9, lines 66-67 and column 10, lines 1-7); providing for the prepending of the first receipt information at a beginning portion of the original electronic record (column 5, lines 55-67 and column 6, lines 1-13); providing for the generation of at least some first identifying information, wherein the first identifying information includes a provable representation of the first receipt information (column 3, lines 12-21); providing for the appending of the first identifying information at an end portion of the original electronic record (column 3, lines 33-35); providing for the storage of the original electronic record with the prepended first receipt information and the appended first identifying information in the repository as an authoritative electronic record; providing for the receipt of a request to review and optionally sign the authoritative electronic record at a remote location; providing for the computation of a complement of the proper subset of the authoritative electronic record; and transmitting the

complement of the proper subset of the authoritative electronic record to the remote location ( column 6, lines 14-59 and column 9, lines 27-41);providing for the display of the complement of the proper subset of the authoritative electronic record at the remote location; providing for at least some digital signature information to be generated at the remote location using the computed message digest and a private key (column 10, lines 23-49); providing for the receipt of the digital signature information in the repository; providing for the generation of at least some second receipt information, wherein the second receipt information includes information relating to the signed authoritative electronic record (column 3, lines 12-21); providing for the prepending of the second receipt information at a beginning portion of the signed authoritative electronic record (column 3, lines 23-37); providing for the generation of at least some second identifying information, wherein the second identifying information includes a provable representation of the receipt information; providing for the appending of the second identifying information at an end portion of the signed authoritative electronic record; providing for the determination of whether the digital signature information represents a valid digital signature (column 3, lines 23-37); and providing for the amending, if the digital signature information is determined to represent a valid digital signature, of the authoritative electronic record in the repository to include the digital signature information, the prepended second receipt information, and the appended second identifying information from the signed authoritative electronic record (column6, lines 31-59). Bisbee does not

explicitly teach providing for the computation of a partial message digest of a proper subset of the authoritative electronic record; providing for the transmission of the partial message digest and providing for the computation of a message digest, at the remote location, using the partial message digest and the complement of the proper subset of the authoritative electronic record. However, in an analogous art, Vanstone teaches providing for the computation of a partial message digest of a proper subset of the authoritative electronic record; providing for the transmission of the partial message digest and providing for the computation of a message digest, at the remote location, using the partial message digest and the complement of the proper subset of the authoritative electronic record (column 3, lines 55-67 and column 4, lines 1-26). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Bisbee's method to include providing for the computation of a partial message digest of a proper subset of the authoritative electronic record; providing for the transmission of the partial message digest and providing for the computation of a message digest, at the remote location, using the partial message digest and the complement of the proper subset of the authoritative electronic record. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to confirm authenticity, insure the accuracy of the message and furthermore to protect the individual blocks of data from any alteration (column 2, lines 45-49).

**Regarding claim 22**

Bisbee teaches a method for displaying a provable representation of an authoritative electronic record at a remote location, the method comprising the steps of: receiving a request to review and optionally sign an authoritative electronic record stored in a repository, at a remote location, wherein the authoritative electronic record includes at least some first receipt information prepended at a beginning portion of the authoritative electronic record, and at least some first identifying information, appended at an end portion of the original electronic record, wherein the first identifying information includes a provable representation of the first receipt information (column 6, lines 14-59 and column 9, lines 27-41); computing a complement of the proper subset of the authoritative electronic record (column 9, lines 27-41), allowing a message digest to be computed, at the remote location, using the partial message digest and the complement of the proper subset of the authoritative electronic record; and allowing the complement of the proper subset of the authoritative electronic record to be displayed at the remote location, wherein the complement of the proper subset of the authoritative electronic record is a provable representation of the authoritative electronic record (column 10, lines 23-49). Bisbee does not explicitly teach computing a partial message digest of a proper subset of the authoritative electronic record; transmitting the partial message digest of the authoritative electronic record to the remote location and transmitting the complement of the proper subset of the authoritative electronic record to the

remote location. However, in an analogous art, Vanstone teaches computing a partial message digest of a proper subset of the authoritative electronic record (column 3, lines 20-53); transmitting the partial message digest of the authoritative electronic record to the remote location and transmitting the complement of the proper subset of the authoritative electronic record to the remote location (column 3, lines 55-67 and column 4, lines 1-26). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Bisbee's method to include computing a partial message digest of a proper subset of the authoritative electronic record; transmitting the partial message digest of the authoritative electronic record to the remote location and transmitting the complement of the proper subset of the authoritative electronic record to the remote location. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to confirm authenticity, insure the accuracy of the message and furthermore to protect the individual blocks of data from any alteration (column 2, lines (45-49).

### **Regarding claim 30**

Bisbee teaches a method for generating a digital signature at a remote location and transmitting the digital signature to a repository, the method comprising the steps of: computing a message digest of the authoritative electronic record using the complement of the proper subset of the authoritative

electronic record and the partial message digest of the authoritative electronic record; allowing a private key to be used to generate at least some digital signature information; and transmitting the digital signature information to the repository (column 10, lines 23-49). Bisbee does not explicitly teach receiving a complement of the proper subset of the authoritative electronic record from a repository; receiving a partial message digest of the authoritative electronic record from a repository. However, in an analogous art, Vanstone teaches receiving a complement of the proper subset of the authoritative electronic record from a repository; receiving a partial message digest of the authoritative electronic record from a repository (column 3, lines 55-67 and column 4, lines 1-26). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Bisbee's method to include receiving a complement of the proper subset of the authoritative electronic record from a repository; receiving a partial message digest of the authoritative electronic record from a repository. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to confirm authenticity, insure the accuracy of the message and furthermore to protect the individual blocks of data from any alteration (column 2, lines 45-49).

**Regarding claim 31**

Bisbee teaches a method for including a valid digital signature in an authoritative electronic record stored in a repository, wherein the authoritative electronic record includes at least some first receipt information prepended at a beginning portion of the authoritative electronic record (column 5, lines 55-67 and column 6, lines 1-13), and at least some first identifying information appended at an end portion of the authoritative electronic record (column 3, lines 33-35), wherein the first identifying information includes a provable representation of the first receipt information (column 3, lines 12-21), the method comprising the steps of: receiving at least some digital signature information, wherein the digital signature information was generated using a private key and a message digest (column 10, lines 33-43), determining whether the digital signature information represents a valid digital signature; and amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the digital signature information (column 6, lines 31-59). Bisbee does not explicitly teach the message digest is computed using a partial message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record. However, in an analogous art, Vanstone teaches the message digest is computed using a partial message digest of the authoritative electronic record and a complement of a proper subset of the

authoritative electronic record (column 3, lines 55-67 and column 4, lines 1-26).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Bisbee's method to include the message digest computed by using a partial message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to confirm authenticity, insure the accuracy of the message and furthermore to protect the individual blocks of data from any alteration (column 2, lines 45-49).

### **Regarding claim 36**

Bisbee teaches a computer system for maintaining and updating a unique authoritative electronic record, the system comprising: means for receiving an original electronic record means for generating at least some first receipt information, wherein the first receipt information includes information relating to the original electronic record (column 9, lines 66-67 and column 10, lines 1-7); means for prepending the first receipt information at a beginning portion of the original electronic record (column 5, lines 55-67 and column 6, lines 1-13); means for generating at least some first identifying information, wherein the first identifying information induces a provable representation of the first receipt information (column 3, lines 12-21); means for appending the first identifying

information at an end portion of the original electronic record (column 3, lines 33-35); means for storing the original electronic record with the prepended first receipt information and the appended first identifying information in the repository as an authoritative electronic record; means for receiving a request to review and optionally sign the authoritative electronic record at a remote location; means for computing a complement of the proper subset of the authoritative electronic record; and means for transmitting the complement of the proper subset of the authoritative electronic record to the remote location (column 6, lines 14-59 and column 9, lines 27-41); means for displaying the complement of the proper subset of the authoritative electronic record at the remote location; means for allowing at least some digital signature information to be generated at the remote location, wherein the digital signature information is generated using the computed message digest and a private key (column 10, lines 23-49); means for receiving the digital signature information in the repository; means for generating at least some second receipt information, wherein the second receipt information includes information relating to the signed authoritative electronic record (column 3, lines 12-21); means for prepending the second receipt information at a beginning portion of the signed authoritative electronic record; means for generating at least some second identifying information, wherein the second identifying information includes a provable representation of the receipt information; means for appending the second identifying information at an end portion of the signed authoritative electronic record; means for determining

whether the digital signature information represents a valid digital signature (column 3, lines 23-37); and means for amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record in the repository to include the digital signature information, the prepended second receipt information, and the appended second identifying information from the signed authoritative electronic record (column 6, lines 31-59). Bisbee does not explicitly teach means for computing a partial message digest of a proper subset of the authoritative electronic record; means for transmitting the partial message digest and means for computing a message digest, at the remote location, using the partial message digest and the complement of the proper subset of the authoritative electronic record. However, in an analogous art, Vanstone teaches means for computing a partial message digest of a proper subset of the authoritative electronic record; means for transmitting the partial message digest and means for computing a message digest, at the remote location, using the partial message digest and the complement of the proper subset of the authoritative electronic record (column 3, lines 55-67 and column 4, lines 1-26). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Bisbee's computer system to include means for computing a partial message digest of a proper subset of the authoritative electronic record; means for transmitting the partial message digest and means for computing a message digest, at the remote location, using the partial message digest and the complement of the proper subset of the

authoritative electronic record. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to confirm authenticity, insure the accuracy of the message and furthermore to protect the individual blocks of data from any alteration (column 2, lines 45-49).

**Regarding claim 38**

Bisbee teaches a system for obtaining a digital signature on an authoritative electronic record stored in a repository, the system comprising: a software program that is capable of receiving a request to review and optionally sign an authoritative electronic record, stored in a repository, at a remote location, wherein the authoritative electronic record includes at least some first receipt information prepended at a beginning portion of the authoritative electronic record, and at least some first identifying information, appended at an end portion of the authoritative electronic record, wherein the first identifying information includes a provable representation of the first receipt information (column 6, lines 14-59 and column 9, lines 27-41); a software program that is capable of allowing the complement of the proper subset of the authoritative electronic record to be displayed at the remote location; and a software program that is capable of allowing at least some digital signature information to be generated using the computed message digest and a private key; a software program that is capable of computing a complement of the proper subset of the

authoritative electronic record (column 10, lines 23-49). Bisbee does not explicitly teach a software program that is capable of computing a partial message digest of a proper subset of the authoritative electronic record; a software program that is capable of controlling the transmission of the complement of the proper subset of the authoritative electronic record, the partial message digest and the complement of the proper subset of the authoritative electronic record to the remote location; a software program that is capable of allowing a message digest to be computed, at the remote location, using the partial message digest and the complement of the proper subset of the authoritative electronic record. However, in an analogous art, Vanstone teaches a software program that is capable of computing a partial message digest of a proper subset of the authoritative electronic record; a software program that is capable of controlling the transmission of the complement of the proper subset of the authoritative electronic record, the partial message digest and the complement of the proper subset of the authoritative electronic record to the remote location; a software program that is capable of allowing a message digest to be computed, at the remote location, using the partial message digest and the complement of the proper subset of the authoritative electronic record (column 3, lines 55-67 and column 4, lines 1-26). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Bisbee's system to include a software program that is capable of computing a partial message digest of a proper subset of the authoritative electronic record; a

software program that is capable of controlling the transmission of the complement of the proper subset of the authoritative electronic record, the partial message digest and the complement of the proper subset of the authoritative electronic record to the remote location; a software program that is capable of allowing a message digest to be computed, at the remote location, using the partial message digest and the complement of the proper subset of the authoritative electronic record. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to confirm authenticity, insure the accuracy of the message and furthermore to protect the individual blocks of data from any alteration (column 2, lines 45-49).

**Regarding claim 39**

Bisbee teaches a system for including a valid digital signature in an authoritative electronic record stored in a repository, wherein the authoritative electronic record includes at least some first receipt information prepended at a beginning portion of the authoritative electronic record (column 5,lines 55-67 and column 6,lines 1-13), and at least some first identifying information appended at an end portion of the authoritative electronic record, (column 3, lines 33-35) wherein the first identifying information includes a provable representation of the first receipt information (column 3,lines 12-21), the system comprising: a software program that is capable of receiving at least some digital signature information

produced using a computed message digest and a private key (column 10, lines 33-43), a software program that is capable of determining whether the digital signature information represents a valid digital signature; a software program that is capable of amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record includes the authoritative electronic record and the digital signature information (column 6, lines 31-59); and a software program that is capable of storing the signed authoritative electronic record in the repository as the authoritative electronic record (column 10, lines 1-7). Bisbee does not explicitly teach the computed message digest is generated using a partial message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record. However, in an analogous art, Vanstone teaches the computed message digest is generated using a partial message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record (column 3, lines 55-67 and column 4, lines 1-26). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Bisbee's system to include the computed message digest is generated using a partial message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to

do so in order to confirm authenticity, insure the accuracy of the message and furthermore to protect the individual blocks of data from any alteration (column 2, lines 45-49).

**Regarding claim 40**

Bisbee teaches a computer program product for obtaining a digital signature on a single authoritative copy of an original electronic record comprising: a computer usable medium and computer readable code embodied on the computer usable medium for obtaining a digital signature on a single authoritative copy of an original electronic record (column 8, lines 39-54), the computer readable code comprising: computer readable program code devices configured to cause the computer to effect the storing of an original electronic record as an authoritative electronic record in a repository (column 10, lines 1-8); computer readable program code devices configured to cause the computer to effect the generation of at least some digital signature information, wherein the digital signature information is produced using a computed message digest and a private key (column 10, lines 23-49), computer readable program code devices configured to cause the computer to effect the transmission of the digital signature information from the remote location to the repository and the receipt of the digital signature information in the repository; computer readable program code devices configured to cause the computer to effect the amending, if the received digital signature information is determined to be valid, of the

authoritative electronic record in the repository to include at least some of the received digital signature information (column 6, lines 14-59). Bisbee does not explicitly teach the computer readable program code devices configured to cause the computer to effect the transmission of a provable representation of an authoritative electronic record from a repository to a remote location, wherein the provable representation of the authoritative electronic record includes a partial message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record and the computed message digest is generated using the partial message digest of the authoritative electronic record and the complement of a proper subset of the authoritative electronic record. However, in an analogous art, Vanstone teaches a computer readable program code devices configured to cause the computer to effect the transmission of a provable representation of an authoritative electronic record from a repository to a remote location, wherein the provable representation of the authoritative electronic record includes a partial message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record and the computed message digest is generated using the partial message digest of the authoritative electronic record and the complement of a proper subset of the authoritative electronic record (column 3, lines 55-67 and column 4, lines 1-26). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Bisbee's computer program to include a computer readable program code

devices configured to cause the computer to effect the transmission of a provable representation of an authoritative electronic record from a repository to a remote location, wherein the provable representation of the authoritative electronic record includes a partial message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record and the computed message digest is generated using the partial message digest of the authoritative electronic record and the complement of a proper subset of the authoritative electronic record. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to confirm authenticity, insure the accuracy of the message and furthermore to protect the individual blocks of data from any alteration (column 2, lines 45-49).

### **Regarding claims 2 and 18**

Bisbee and Vanstone teach all limitation of the claim as applied to claims 1 and 17 above. Bisbee furthermore teaches a method, wherein the step of receiving an original electronic record further comprises the step of adding time-stamp information to the original electronic record, wherein the time-stamp information comprises the time and the date when the original electronic record is received in the repository (column 3, lines 48-55).

**Regarding claims 3 and 19**

Bisbee and Vanstone teach all limitation of the claim as applied to claims 1 and 17 above. Bisbee furthermore teaches a method, wherein the digital signature information is created with the use of the message digest and a private key (column 10, lines 33-43).

**Regarding claims 4, 20 and 27**

Bisbee and Vanstone teach all limitation of the claim as applied to claims 1, 17 and 22 above. Bisbee furthermore teaches a method, wherein the first receipt information includes at least some digital signature information that is generated using a private key of the repository (column 10, lines 33-43).

**Regarding claim 5, 6, 23 and 24**

Bisbee and Vanstone teach all limitation of the claim as applied to claims 1 and 22 above. Bisbee furthermore teaches a method, wherein the proper subset of the authoritative electronic record comprises information prepended to beginning portion of the authoritative electronic record (column 5, lines 56-67 and column 6, lines 1-13) and the complement of the proper subset of the authoritative electronic record comprises the original electronic record and information appended to the end portion of the original electronic record (column 10, lines 53-61).

**Regarding claims 7 and 25**

Bisbee and Vanstone teach all limitation of the claim as applied to claims 1 and 22 above. Bisbee furthermore teaches a method, wherein the steps of transmitting the partial message digest of the authoritative electronic record and transmitting the complement of the proper subset of the authoritative electronic record to the remote location include transmitting the partial message digest and transmitting the complement of the proper subset of the authoritative electronic record to the remote location in a single transmission (column 9, lines 27-41).

**Regarding claims 8 and 28**

Bisbee and Vanstone teach all limitation of the claim as applied to claims 1 and 22 above. Bisbee furthermore teaches a method; wherein at least one software program associated with the repository is utilized at the remote location (column 8, lines 20-39).

**Regarding claims 9 and 35**

Bisbee and Vanstone teach all limitation of the claim as applied to claims 1 and 34 above. Bisbee furthermore teaches a method, wherein the partial message digest includes information necessary to compute the message digest at the remote location (column 10, lines 23-49).

**Regarding claim 10**

Bisbee and Vanstone teach all limitation of the claim as applied to claim 1 above. Bisbee furthermore teaches a method, wherein the step of prepending the second receipt information at a beginning portion of the signed authoritative electronic record includes replacing the first receipt information with the second receipt information (column 9, lines 66-67 and column 10, lines 1-7).

**Regarding claim 11**

Bisbee and Vanstone teach all limitation of the claim as applied to claim 1 above. Bisbee furthermore teaches a method, wherein the second receipt information includes at least some digital signature information that is generated using a private key of the repository (column 5, lines 64-67 and column 6, lines 1-13).

**Regarding claim 12**

Bisbee and Vanstone teach all limitation of the claim as applied to claim 1 above. Bisbee furthermore teaches a method, wherein the second identifying information is generated using at least some repository information (column 3, lines 23-37).

**Regarding claims 13 and 14**

Bisbee and Vanstone teach all limitation of the claim as applied to claims 1 above. Bisbee furthermore teaches a method, wherein the second identifying information is generated using at least some user information or some remote location information (column 11, lines 12-23).

**Regarding claim 15**

Bisbee and Vanstone teach all limitation of the claim as applied to claim 1 above. Bisbee furthermore teaches a method, wherein the step of appending the second identifying information at an end portion of the signed authoritative electronic record includes amending the first identifying information to include the second identifying information (column 2, lines 30-47).

**Regarding claim 26**

Bisbee and Vanstone teach all limitation of the claim as applied to claim 22 above. Bisbee furthermore teaches a method, wherein the complement of the proper subset of the authoritative electronic record includes a complement of the proper subset of the authoritative electronic record and all information appended to the end portion of the authoritative electronic record (column 10, lines 53-61).

**Regarding claim 29**

Bisbee and Vanstone teach all limitation of the claim as applied to claim 22 above. Bisbee furthermore teaches a method, further comprising the step of allowing at least the digital signature information to be returned to the repository (column 3, lines 12-21).

**Regarding claim 32**

Bisbee and Vanstone teach all limitation of the claim as applied to claim 31 above. Bisbee furthermore teaches a method, wherein the step of amending, if the digital signature information is determined to represent a valid digital signature, a signed authoritative electronic record includes the steps of: prepending digital signature information comprising a digital signature to the beginning portion of the authoritative electronic record; and appending digital signature information comprising a provable representation of the digital signature information to the end portion of the authoritative electronic record (column 10, lines 33-61).

**Regarding claim 33**

Bisbee and Vanstone teach all limitation of the claim as applied to claim 31 above. Bisbee furthermore teaches a method, wherein the step of amending, if the digital signature information is determined to represent a valid digital signature, a signed authoritative electronic record includes the steps of:

prepending at least some signature receipt information to the beginning portion of the authoritative electronic record, wherein the signature receipt information comprises a unique representation of the signed authoritative electronic record; and appending at least some identifying information to the end portion of the authoritative electronic record, wherein the identifying information comprises a provable representation of the signature receipt (column 3, lines 12-35).

**Regarding claim 34**

Bisbee and Vanstone teach all limitation of the claim as applied to claim 31 above. Bisbee furthermore teaches a method, further including the steps of: receiving a request, from a remote location, to review and optionally sign the signed authoritative electronic record, wherein the signed authoritative electronic record includes validated digital signature information (column 6, lines 14-30); computing a complement of the proper subset of the signed authoritative electronic record; transmitting the complement of the proper subset of the signed authoritative electronic record to the remote location ( column 6, lines 14-59 and column 9, lines 27-41); allowing the complement of the proper subset of the signed authoritative electronic record to be displayed at the remote location (column 10, lines 23-49).; receiving at least some new digital signature information, wherein the new digital signature information was generated using a private key and the computed message digest (column 10, lines 33-43); determining whether the new digital signature information represents a valid

digital signature; and amending, if the new digital signature information is determined to represent a valid digital signature, the signed authoritative electronic record to include the new digital signature information (column 10, lines 23-33). Vanstone furthermore teaches computing a partial message digest of a proper subset of the signed authoritative electronic record; transmitting the partial message digest of the signed authoritative electronic record to the remote location; allowing a message digest to be computed, at the remote location, using the partial message digest and the complement of the proper subset of the signed authoritative electronic record (column 3, lines 55-67 and column 4, lines 1-26).

#### **References Cited, Not Used**

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

1. U.S. Patent No. 5,347,581

This reference relates to a system for improving the computational efficiency of digital signature algorithm.

2. U.S. Patent No. 5,633,931

This reference relates to authenticating message signature.

3. U.S. Patent No. 6,237,096

This reference relates to systems and methods for providing a

verifiable chain of evidence and security for the transfer and retrieval of documents in digital formats.

### Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300 Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER

Ali Abyaneh A.A  
Patent Examiner  
Art Unit 2137  
11/16/05